Вестник УрФО № 1(23) / 2017, с. 4–9

УДК 004.056.53 + 336.717.111.7:004.738.5.056

Григоров А. С.

ИСПОЛЬЗОВАНИЕ АНАЛИЗА SQL-ЗАПРОСОВ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА СИСТЕМЫ МОБИЛЬНОГО БАНКИНГА

В данной статье рассмотрены основные типы уязвимостей приложений мобильного банкинга и возможные атаки в разрезе функциональности приложений и типов интеграционных сервисов на стороне серверного ПО систем мобильного банкинга. Предложен метод обнаружения некоторых уязвимостей на основе анализа SQL-запросов, выполняемых к СУБД системы дистанционного банковского обслуживания (ДБО), дающий дополнительные возможности качественно снизить количество ложноположительных и ложноотрицательных ошибок обнаружения мошеннических операций в системах ДБО. Даны рекомендации по организации процесса разработки систем мобильного банкинга, позволяющие снизить риск возникновения уязвимостей в создаваемых системах.

Ключевые слова: *мобильный банкинг, системы противодействия мошенничеству, обнаружение аномалий, SQL, СУБД.*

Grigorov A. S.

USING THE ANALYSIS OF SQL-QUERIES TO DETECT ATTACKS ON MOBILE BANKING SYSTEM

This paper describes the main types of mobile banking application vulnerabilities and possible attacks in the context of the functionality of applications and types of integration services on the side of the server software of mobile banking system. Propose the method for detecting certain vulnerabilities by analyzing the SQL-queries performed to the database of e-banking system (RBS), which gives additional opportunities to reduce false positives and false negative error detection of fraudulent transactions in RBS systems. This paper also provides recommendations of the organization of the development process of mobile banking systems that reduce the risk of vulnerabilities in established systems.

Keywords: *mobile banking, anti-fraud system, anomaly detection, SQL, RDBMS.*

Согласно результатам исследования[1], проведённого «Markswebb Rank & Report» в ноябре-декабре 2015 года, мобильными банковскими приложениями для смартфонов и планшетов в Российской Федерации пользуются 18,1 млн. человек, что составляет 33% российской интернет-аудитории. В 2014 году оборот на российском рынке мобильного банкинга составил 15 млрд. рублей[8], при этом по прогнозам «J'son & Partners Consulting» среднегодовой темп роста с 2014 по 2018 года составит 28%. В тоже время результат анализа мобильных приложений российских банков[7] показывает, что разработчики мобильных приложений не уделяют должного внимания вопросам безопасности и не следуют рекомендациям по безопасной разработке под конкретные мобильные операционные системы. При этом стоит отметить, что список уязвимостей приложений мобильного банкинга во многом схож со списком уязвимостей мобильных приложений в целом[7], представленным в отчёте OWASP Top 10 Mobile Risks 2014[3]. Это позволяет говорить о потенциальной возможности выполнения широко распространённых атак на мобильные банковские приложения без знания специфики их работы, что снижает требования к навыкам злоумышленников для осуществления успешной атаки.

В данной статье будут рассмотрены основные типы уязвимостей приложений мобильного банкинга и представлена карта возможных атак в разрезе функциональности приложений и типов интеграционных сервисов на стороне серверного ПО систем мобильного банкинга. Также будет предложен метод обнаружения некоторых уязвимостей на основе анализа SQL-запросов, выполняемых к СУБД системы дистанционного банковского обслуживания (ДБО).

Организация серверной части системы мобильного-банкинга

В настоящий момент возможности мобильных операционных систем не ограничивают разработчиков, позволяя создавать сервисы, не уступающие по функциональности традиционным интернет-банкам. Если ранее банки через мобильные приложения предоставляли в первую очередь информационные сервисы, такие как просмотр списка счётов, получение информации о проведённых транзакциях или просмотр остатка на карточном счёте, то сейчас ситуация существенно изменилась. Преследуя цели сокращения операционных издержек, расширения клиентской базы и увеличения комиссионных доходов, банки стремятся нарастить функциональные возможности дистанционных сервисов, в частности добавляя возможность выполнения платежных операций, P2P-переводов, операций онлайн-кредитования. Однако, помимо удобства для клиентов банка, возрастает угроза кражи денежных средств.

Типичным вариантом организации работы приложений мобильного банкинга является подход, когда на стороне сервера ДБО определяется набор сервисов, к которым приложение мобильного банка выполняет обращение через интернет. Взаимодействие между мобильным приложением и сервером может быть построено на основе RESTful вебсервисов, протокола SOAP или других подходов, работающих поверх HTTP. Мобильное приложение выступает инициатором взаимодействия, отправляя запрос, а сервер системы ДБО выполняет запрашиваемое действие и возвращает ответ. В зависимости от используемой технологий, форматы передачи данных запросов и ответов могут быть разными, наиболее распространенными являются XML и JSON.

Набор прикладных сервисов и операций, которые входят в API системы ДБО для мобильных платформ, зависит о специфики конкретных систем и функциональности разрабатываемых мобильных приложений. Типовой набор бизнес операций, доступный в приложениях мобильного банкинга для физических лиц от ведущих российских компаний разработчиков систем ДБО, можно по функциональному назначению разделить на несколько групп[2,10]:

1. Сервисы авторизации и безопасности:

– аутентификация клиента по логину и паролю;

– завершение текущей сессии;

– смена пароля для доступа к системе ДБО;

– регистрация мобильного устройства, привязка устройства к учётной записи клиента банка;

– получение паролей 3-D Secure;

– выполнение подтверждения корректности введённых реквизитов платежных распоряжений и заявок.

2. Информационные сервисы:

– получение списков текущих счетов,

карт, вкладов, кредитов, металлических счётов, а также их основных атрибутов (номера счетов, остатки на счетах, тарифные планы);

– получение реквизитов пополнения текущих, карточных, депозитных счетов, а также реквизитов для погашения кредита;

– получение графика платежей по кредиту;

– получение выписок по счетам и списков последних транзакций по карте (включая находящихся на исполнении), анализ расходов;

– получение реквизитов виртуальных карт (номер карты, имя владельца, срок действия карты, CVV2/CVC2);

– получение информации об истории операций, выполненных в разных каналах системы ДБО;

– получение анкетных данных клиента для отображения в интерфейсе приложения (ФИО; название отделения банка, в котором обслуживается клиент; номер документа, удостоверяющего личность; ИНН; номера мобильных телефонов и email'ов);

– получение новостной ленты банка, информации о курсах конвертации валют, рекламных предложений, списка банкоматов и офисов банка.

3. Платёжные сервисы:

– выполнение переводов между счетами и картами клиента;

– выполнение внешних переводов по свободным реквизитам, оплата налогов и выполнение платежей в бюджет;

– переводы по номеру карты;

– получение информации о начислениях через систему ГИС ГМП по паспортным данным или ИНН пользователя или уникальному идентификатору начисления;

– оплата услуг, согласно каталогу поставщиков услуг;

– получение списка шаблонов платежей и их выполнение.

4. Сервисы подачи заявок:

– заявки на открытие и закрытие текущих счётов и вкладов;

– заявки на выпуск, блокировку карт (в том числе виртуальных).

Типовые уязвимости систем мобильного банкинга

Атаки на мобильное приложение могут быть выполнены:

– через вредоносное приложение, установленное на том же устройстве, что и приложение мобильного банка;

– путем модификации кода мобильного приложения;

– при наличии контроля канала связи (атака «человек посередине»).

Так согласно исследованию компании Digital Security[7], проведённому в 2013 году, 35% рассмотренных приложений мобильного банкинга, написанных под операционную систему iOS, некорректно организовывали работу с SSL (например, не выполнялась проверка SSL-сертификата банка), что позволяло выполнять перехват и подмену передаваемых данных между приложением и серверной частью. Подмена значений параметров запросов наиболее опасна, так как может привести к исполнению банковских операций с реквизитами, желаемыми злоумышленниками.

Техника защиты серверной части мобильного банка схожа с защитой серверов интернет-банков. Так при разработке серверной части мобильного банкинга следует исходить из того, что любым данным, передаваемым в запросах, нельзя доверять, так как они могут быть подменены злоумышленником. Следовательно, все входные данные должны проходить предварительную проверку. Однако на практике невыполнение или неполное выполнение этих требований не является редкостью: 18% систем ДБО, исследованных компанией Positive Technologies[9], имели уязвимость к SQL-инъекциям. В то же время атаки могут быть выполнены и без применения сложных техник. В случае если на стороне серверной части не выполняется должная проверка связи текущей сессии пользователя с данными, которые передаются в запросе, то, подменив параметры запроса (например, идентификатор счёта назначения перевода), злоумышленник может инициировать выполнение операции, недопустимой с точки зрения бизнес-процессов, заложенных в систему ДБО.

Наличие подобных ошибок в реализации сервисов, относящихся к группе информационных сервисов, а также сервисов получения паролей 3-D Secure, получения списка начислений из ГИС ГМП и получения списков шаблонов платежей может привести к нарушению конфиденциальности данных системы ДБО. В то же время недостаточная обработка входных данных для сервисов из групп «сервисы авторизации и безопасности», «платежные сервисы» и «сервисы подачи заявок» может привести к атакам на целостность и до-

ступность данных в информационных системах банка.

Стоит отметить, что причиной подобных ошибок может являться отсутствие упоминания необходимости проверки входных данных сервисов в функциональных требованиях и технических заданиях на разработку систем. Это приводит к тому, что разработчики не реализуют обработку входных данных, так как это явно не указано в техническом задании, а при функциональном тестировании не рассматриваются сценарии выполнения нелегитимных запросов. Как следствие, существующая уязвимость на этапе тестирования не обнаруживается, и разработанная система запускается в промышленное использование вместе с ней. В качестве возможной меры по уклонению от подобных рисков может являться обязательное выполнение тестирования на проникновение перед запуском системы в промышленное использование, а также использование специализированных систем обнаружения мошеннических операций, которые выполняют анализ операций, проводимых в системах ДБО.

Обнаружения вторжений и мошеннических операций в системах ДБО

На рисунке 1 приведена схема организации работы системы ДБО совместно с системой обнаружения вторжений и мошеннических операций. Принцип работы системы обнаружения вторжений (СОВ) заключается в том, что СОВ анализирует события, происходящие в банковских системах, и в случае обнаружения отклонения работы этих систем от предопределённых шаблонов нормального поведения выполняет информирование специалистов службы безопасности банка (через e-mail, SMS, административную консоль СОВ) или осуществляет активные действия по предотвращению выполнения операции (например, выполняется блокировка учётной записи пользователя или отказ в выполнении операции).

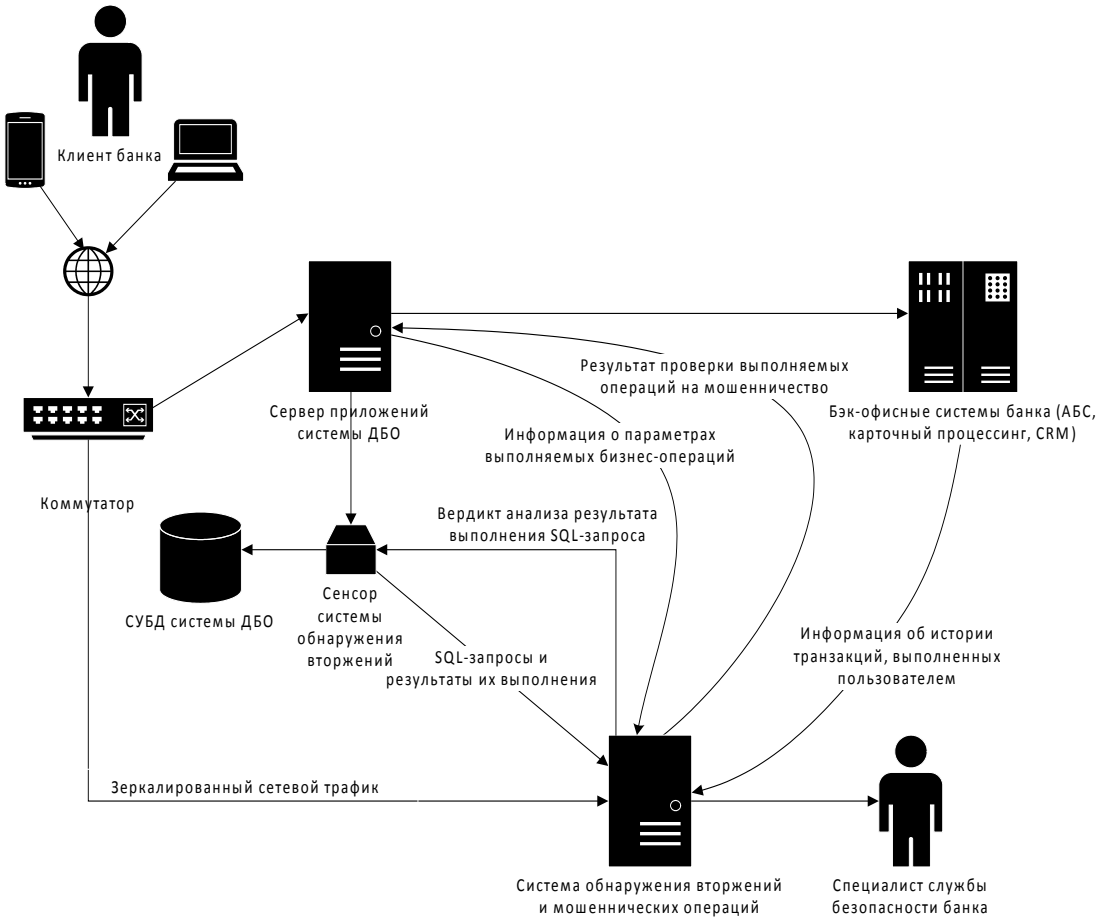

Рис. 1 Схема организации обнаружения мошеннических операций в действиях пользователей системы ДБО

Современные СОВ для анализа событий, происходящих в защищаемой информационной системе, могут агрегировать данные из различных источников. Например, СОВ может анализировать зеркалированный сетевой трафик, идущий к серверам системы ДБО. Однако разработка правил проверки сетевого трафика может потребовать высоких временных и финансовых затрат, связанных с выполнением реверс-инжиниринга используемых протоколов. Для выполнения более качественного анализа современные СОВ могут обмениваться с системой ДБО сообщениями, содержащими информацию о параметрах выполняемых бизнес-операций. Так, например, система ДБО может передать СОВ информацию о реквизитах платежа, IP-адресе и IMEI смартфона, с которого выполняется платёж. СОВ же в свою очередь выполняет проверку переданных данных по набору правил и алгоритмов и выставляет итоговую оценку, на основе которой принимается решение, аномальна ли выполняемая операция или типична для данного пользователя. Организация такого взаимодействия между системой ДБО и СОВ требует специальной доработки системы ДБО, что влечёт за собой дополнительные затраты.

Так как большинство систем ДБО используют для хранения данных реляционные СУБД, а основным средством коммуникации являются SQL-запросы, то альтернативным вариантом можно предложить использовать для получения дополнительных данных о семантике выполняемых пользователем операций анализ выполняемых SQL-запросов и получаемых результатов. При этом, используя подход экранирования драйверов БД[6], можно организовать интеграцию СОВ и защищаемой информационной системы (ИС) без необходимости выполнения доработок на стороне ИС и СУБД.

Автором данной статьи разработан метод обнаружения аномального поведения пользователей ИС на основе оценки результата выполнения SQL-запросов, которые ИС инициировала к СУБД, обрабатывая команды от пользователя[5]. Принятие решения о допустимости выполняемой операции осуществляется путём сравнения полученной выборки данных с ожидаемым результатом, который соответствует профилю нормального поведения пользователя базы данных. Профиль представляет собой граф, отражающий взаимосвязи между данными, которые выбираются SQL-запросами, считающимися допустимыми для нормальной работы пользователя. Использование данного подхода позволяет обнаруживать как атаки на основе SQL-инъекций, так и попытки эксплуатации возможных уязвимостей, связанных с недостаточной проверкой разграничения прав доступа в прикладном коде информационной системы[4].

Метод обнаружения аномального поведения пользователя на основе оценки результатов выполнения SQL-запросов может использоваться для обнаружения атак на сервисы системы ДБО, реализация бизнес-логики которых подразумевает обращение к БД за данными с использованием значений параметров вызова сервисов в качестве аргументов условий SQL-выражений. К таким сервисам, в частности, относятся сервисы выполнения платежей и переводов, получения паролей 3-D Secure и реквизитов виртуальных карт, сервисы получения информации по банковским продуктам клиента, сервисы подачи заявок на открытие или закрытие вклада, выпуск карты.

Рассмотрим, например, сервис открытия вклада, который в качестве входных параметров получает идентификатор счёта клиента, с которого будет выполнен перевод начальной суммы вклада, значение начальной суммы, идентификатор связанного счёта для выплаты процентов и другие параметры открываемого вклада. Злоумышленник может предпринять атаку, пытаясь, например, подменить идентификатор счёта списания на идентификатор счёта, принадлежащего другому клиенту, для того чтобы открыть вклад за счёт средств другого клиента. Или же, наоборот, выполняя атаку «человек посредине», злоумышленник может осуществить подмену идентификатора счёта зачисления процентов для того, чтобы впоследствии проценты по вкладу переводились на нужный ему счёт. При обработке вызова сервиса система ДБО выполняет запрос к БД на получение информации о требующихся счетах. Запрос может иметь следующий вид:

select * from accounts where id in (123, 456);

Согласно разработанному методу[5] данным, полученным в результате выполнения запроса, ставится в соответствие граф, отражающий взаимосвязи между данными попавшими в результат выборки с учётом информации о том, от имени какого пользователя выполнялся запрос. Так каждой записи соответ-

ствует вершина в графе, а вес ребра между двумя вершинами графа равен вероятностьи совместного появления соответствующих записей в результате выполнения SQL-запросов, характерных для нормального поведения пользователя. В дальнейшем на основе рассчитанных характеристик графа, таких как модульность или плотность рёбер, принимается решение о признании результата ожидаемым или аномальным.

Заключение

Ежегодный рост количества пользователей дистанционных сервисов банка, в частности сервисов мобильного банкинга, ставит перед банками новые задачи по обеспечению безопасности использования предоставляемых сервисов. Один из эшелонов защиты систем ДБО – системы обнаружения вторжений и мошеннических операций. В данной статье был предложен вариант использования анализа SQL-запросов, выполняемых системой ДБО, в качестве дополнительного источника информации для принятия решения о подозрительности выполняемых операций. Как следствие, появляются дополнительные возможности качественно снизить количество ложноположительных и ложноотрицательных ошибок обнаружения мошеннических операций.

Примечания

1. e-Finance User Index 2016. [Электронный ресурс]. Режим доступа: http://markswebb.ru/e-finance/e-finance-user-index-2016/. Дата обращения: 13.03.2016.

2. InterBank Mobile Retail // R-Style Softlab: сайт [Электронный ресурс]. Режим доступа: http://softlab.ru/solutions/interbank/5224/

3. Top 10 Mobile Risks. [Электронный ресурс]. Режим доступа: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks. Дата обращения: 13.03.2016.

4. Беляев А.В. Обнаружение атак на базы данных на основе оценки внутренней структуры результатов выполнения SQL-запросов. / А.В. Беляев, А.С. Григоров // Научно-технический вестник Поволжья. №2 2012 г. - Казань: Научно-технический вестник Поволжья, 2012. – С. 99-104.

5. Григоров А.С., Плашенков В.В. Метод обнаружения аномалий в поведении пользователей на основе оценки результатов выполнения SQL-запросов / А.С. Григоров, В.В. Плашенков // Вестник компьютерных и информационных технологий. – 2013. – №3 – С. 49-54.

6. Григоров А.С. О способе интеграции системы обнаружения аномалий в SQL запросах к базе данных на основе результатов выполнения запроса с приложениями, использующими СУБД в качестве хранилища данных [Текст] / А.С. Григоров // Молодой ученый. — 2011. — №12. Т.1. — С. 21-24.

7. Миноженко А. Безопасность мобильных банковских приложений. / А. Миноженко // Information Security / Информационная безопасность. №4, 2013 – С. 30-32.

8. Мобильный банкинг в РФ: прогнозы рынка, поведение пользователей, рейтинг приложений. [Электронный ресурс]. Режим доступа: http://json.tv/ict_telecom_analytics_view/mobilnyy-banking-v-rf-prognozy-rynka-povedenie-polzovateley-reyting-prilojeniy-20150525095123. Дата обращения: 13.03.2016.

9. Статистика уязвимостей систем дистанционного банковского обслуживания (2011-2012). [Электронный ресурс]. Режим доступа: http://www.ptsecurity.ru/download/Analitika_DBO.pdf. Дата обращения: 05.04.2016.

10. Универсальный мобильный клиент. // Компания БСС: сайт [Электронный ресурс]. Режим доступа: http://www.bssys.com/solutions/financial-institutions/dbo-bs-client-chastnyy-klient/chk-mobilnyy-klient/

ГРИГОРОВ Андрей Сергеевич, старший преподаватель, кафедра инфокоммуникационных технологий и безопасности, ФГБОУ ВПО «Череповецкий государственный университет». 162602, г. Череповец, Советский пр-т, д. 8. E-mail: andreygrigorov1986@gmail.com

GRIGOROV Andrey, is a senior lecturer, Department of Information and Communication Technology and Security, Federal State Budget Educational Institution of Higher Education «Cherepovets State University». 162602, Cherepovets, Sovetsky ave., h.8. E-mail: andreygrigorov1986@gmail.com